KING & SPALDING, LLP

191 Peachtree Street
Atlanta, Georgia 30303-1763
Telephone: 404/572-4600
Facsimile: 404/572-5100
www.kslaw.com

FAX TRANSMITTAL SHEET

October 21, 2005

TO:	Examiner C. Colin GAU 2136 U.S. Serial No. 09/665,018	**Company:**	U.S. Patent and Trademark Office
Fax #:	571-273-8300	**City/State:**	Alexandria, VA 22313
	Mail Stop Amendment		
FROM:	Steven P. Wigmore 5551	**Our Ref. #:**	05456.105007

NUMBER OF PAGES (including transmittal sheet): 8

If transmission problems occur or you are not the intended recipient, please call 404.572.2459 immediately. Thank you.

Notes/Comments:

Documents Submitted Via Facsimile:

Applicant: Patrick Taylor et al.

Serial No.: 09/665,018

Filed: September 19, 2000

For: Vulnerability Assessment and Authentication of a Computer by a Local Scanner

Papers Faxed: SUPPLEMENTAL SUMMARY OF TELEPHONIC INTERVIEW OF OCTOBER 4, 2005 (7-pgs.).

RECEIVED
CENTRAL FAX CENTER

OCT 21 2005

Patents

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	**Patrick Taylor et al.**	
Serial No.:	**09/665,018**	Confirmation No.: **4902**
Filed:	**September 19, 2000**	GAU: **2136**
Title:	**Vulnerability Assessment and Authentication of A Computer by A Local Scanner**	Examiner: **C. Colin**

SUPPLEMENTAL SUMMARY OF TELEPHONIC INTERVIEW OF OCTOBER 4, 2005 PURSUANT TO M.P.E.P. §713.04 AND IN RESPONSE TO EXAMINER INTERVIEW SUMMARY FORM (PTOL-413) MAILED OCTOBER 12, 2005

MAIL STOP Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

October 21, 2005

Sir:

In response to the Examiner Colin's Interview Summary (FORM PTOL-413) mailed on October 12, 2005 and supplemental to the Applicants' response that was faxed to the U.S. Patent & Trademark Office on October 12, 2005, please enter the following supplemental interview summary and remarks.

While the Applicants believe that their response of October 12, 2005 to the Office Action of July 12, 2005 contains an accurate summary of the telephonic interview that was conducted on October 4, 2005 with Examiner Colin, the Applicants are submitting this supplemental interview summary in order to respond to some points raised by Examiner Colin in his summary that were not discussed during the telephonic interview.

I hereby certify that this correspondence is being facsimile transmitted to: Mail Stop Amendment, The Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, Attn: Examiner C. Colin, GAU 2136, Facsimile No. 571-273-8300, on October 21, 2005.

Steven P. Wigmore, Reg. No. 40,447

The following is copy of the Applicants' Summary (As Provided on pages 8-9 of Applicants Response of October 12, 2005):

Summary of Telephonic Interview of October 4, 2005

The Applicants and the undersigned thank Examiner Colin for his time and consideration given during the telephonic interview of October 4, 2005. During this telephonic interview, a proposed amendment to the claims provided by the Applicants prior to the interview was discussed.

The Applicants' representative explained that the prior art of record does not provide any teaching of generating workstation credentials derived from a scanner conducting the vulnerability assessment of the workstation and where the workstation credentials comprise at least one of information about integrity of the workstation and a security posture of the workstation. It was explained that the prior art does not provide any teaching of comparing the workstation credentials to a workstation policy in order to grant the workstation access to one or more services available on a network server if the workstation credentials are in compliance with the workstation policy.

To emphasize that the prior art of record does not grant access to a network service for a workstation, but instead, only authenticates a user to access a service, the Applicants' representative pointed out that the amended independent claims recite that a request for credentials associated with a user is issued after a workstation is granted access to a service in order to determine if the user is authorized to access the a service available on a network server. This means that each of the independent claims require at least two authentication steps: (1) granting a physical workstation access to a service; and (2) granting a user access to a service if the physical workstation is granted access to the service.

U.S. Patent Application Publication No. 2001/0034847, published in the name of Stephen E. Gaul (hereinafter, the "Gaul reference") may provide a teaching of generating workstation credentials. However, it was explained that this reference does not use these workstation credentials to grant a workstation access to a network service before a request is issued to authenticate a user to determine if a user should be permitted to access the network service.

U.S. Patent No. 6,438,600 issued in the name of Greenfield et al. (hereinafter the "Greenfield reference") describes technology that only authenticates users and not a physical workstation. In other words, the Greenfield reference like the Gaul reference does not provide any teaching of checking workstation credentials associated with the workstation (and not with the user) in order to grant a workstation access to a network service.

Similarly, the printed publication entitled, "White Paper: Secure Computing with Java: Now and the Future," that was published in 1994 and authored by Gary McGraw and owned by Sun Microsystems, Inc. (hereinafter the "McGraw publication") only describes authenticating a user to access a service and not granting a workstation access to a service irrespective of a user.

Examiner Colin indicated that he understood the Applicants' position and that he would consider it when the formal response was filed. The Applicants and the undersigned appreciate the Examiner Colin's time and consideration given during the telephone interview of October 4, 2005.

Supplemental Summary in response to Examiner's Interview Summary (PTOL-413) Mailed on October 12, 2005 - (same day that Applicants' Response was filed):

Examiner Colin notes in his interview summary (on the continuation sheet) that the Applicants will make a further amendment to include language of authentication of the workstation. The Applicants believe that the following language of the independent claims can be interpreted as a form of authentication:

> "granting the workstation access to one or more services available on the network server if the workstation credentials are in compliance with the workstation policy;
> if access to the one or more services available on the network server is granted to the workstation because the workstation credentials are in compliance with the workstation policy,..." See independent Claim 1, for example.

However, if the Examiner does not agree with the Applicants interpretation, then the Examiner is invited to contact the undersigned as the Applicants would approve an

Examiner's amendment to the claims if the actual words, "workstation authentication," are desired by Examiner Colin.

Examiner Colin notes in his interview summary (on the continuation sheet) that, after the telephonic interview with the Applicants' representative, the Examiner wanted to clarify that, "Greenfield [U.S. Patent No. 6,438,600] also presents other embodiment where the machine at which the user requests information is referred as the client (see column 1, lines 39-67) that also needs to be trusted to get access to the server (see column 6, line 49 through column 7, line 30)."

The Applicants agree that a web browser running on a computer remote from a server computer as described in column 1, lines 39-67 by the Greenfield reference may be referred to as a "client." But the Applicants submit that this passage is only describing the conventional three-tiered computer architecture that is known to one of ordinary skill in the art. It is the user or operator that is authenticated in this conventional computer architecture and not the browser or computer itself. This passage does not teach or suggest in any way teach a first step in which a workstation is first authenticated and then a second step in which the user of the workstation is authenticated:

> "The user working in a Web environment will have software running on his computer to allow him to create and send requests for information, and to see the results. These functions are typically combined in what is referred to as a 'Web browser', or 'browser'. After the user has created his request using the browser, the request message is sent out into the Internet for processing. The target of the request message is one of the interconnected computers in the Internet network. That computer will receive the message, attempt to find the data satisfying the user's request, format that data for display with the user's browser, and return the formatted response to the browser software running on the user's computer. This is an example of a client-server model of computing, where the machine at which the user requests information is referred to as the client, and the computer that locates the information and returns it to the client is the server. In the Web environment, the server is referred to as a 'Web server'. The client-server model may be extended to what is referred to as a "three-tier architecture". This architecture places the Web server in the middle tier, where the added third tier typically represents data repositories of

> information that may be accessed by the Web server as part of the task of processing the client's request. This three-tiered architecture recognizes the fact that many client requests do not simply require the location and return of static data, but require an application program to perform processing of the client's request in order to dynamically create the data to be returned. In this architecture, the Web server may equivalently be referred to as an 'application server', reflecting the fact that this middle tier is where the business logic of the application typically resides, and the computers on which the data repositories reside may be referred to as 'data servers', or 'backend data servers'. A data server stores and manages the data that is used by an application." See Greenfield reference, column 1, line 39 through column 2, line 6. Emphasis supplied.

Examiner Colin also refers the Applicants to column 6, line 49 through column 7, line 30 of the Greenfield reference. The Applicants understand this passage to describe security features in the Java computer language in which a browser can down load information from different servers and, as a measure of security, this information from different servers is maintained in different and separate locations, "separate sandboxes," within the client computer running the Java-language based browser:

> "When code is downloaded from a remote source to a client machine, there is the potential for the executable code to perform destructive function when it executes. For example, the code may contain what is called a 'Trojan horse', meaning code that appears to have one function when in fact it also has hidden functions. An example of this type of hidden function is scanning the machine's hard drive for confidential information (such as a credit card number) and then transmitting that information to a computer over the Internet. Or, the downloaded code may contain a virus that could destroy the files on the machine's hard drive. Security concerns such as these are well known.
>
> Java contains built-in security mechanisms that are designed to limit the destructive potential of applets. One of these mechanisms is the 'sandbox' concept, whereby downloaded classes are restricted to accessing system resources (such as applet code and stored data) within their own sandbox. Three system components are involved in implementing the sandbox concept, and are provided as part of a standard Java Development Kit. These

components are: the class loader, the byte-code verifier, and the security manager. In particular, the class loader downloads applets and their corresponding classes into a namespace hierarchy that identifies the server and codebase from which the code (i.e. the applets and classes) was downloaded. A static data area is then allocated for use by the code in that namespace. For example, objects to be used by the classes (such as values for variables) are stored in this static data. As an example of how the sandbox concept operates, suppose two different applets use a class 'myClass' during execution. If both of these applets are downloaded from the same server and codebase, then both applets may share the same instantiation of the code in 'myClass' and the same static data area. If the applets are from different servers and/or codebases, however, the class loader will automatically load a separate instance of 'myClass' for each applet, and these separate instances will not share the same static data area. In this latter situation, each of the applets is being restricted to operation within its own sandbox.

More detailed information on the Java sandbox may be obtained by consulting a Java publication. One publication that discusses the sandbox concept is 'Secure Computing with Ser. No. 09/240,398 Java.TM: 'Now and the Future', and in particular the section thereof entitled 'The Java Sandbox'. This publication is available on the World Wide Web from Sun Microsystems at the address java.sun.com/security/javaone97-whitepaper.html." See column 6, line 49 through column 7, line 30 of the Greenfield reference.

The Applicants do not believe that that second passage of the Greenfield reference listed above, alone or in combination with the first passage of Greenfield noted by Examiner Colin, teach or suggest in any way a first step in which a workstation is first authenticated and then a second step in which the user of the workstation is authenticated.

The Applicants and the undersigned request Examiner Colin to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202.